What is claimed is:

1. A receiver for receiving program content and for displaying said program content under predetermined conditions, wherein

said receiver comprises:

a component identified by a computer readable serial number,

data storage storing access data determining programming to be decrypted by said receiver, a public cryptographic key, a private cryptographic key for decrypting information encrypted with said public cryptographic key, and a code representing said component identifier, and

a signal processor decrypting said encrypted program content in accordance with said access data stored within said data storage; and

a first microprocessor,

said receiver periodically performs a first method comprising:

reading said computer readable serial number;

generating a hash value representing said computer readable serial number, and

storing said hash value in said data storage,

said receiver additionally performs a second method comprising:

reading said hash value from said data storage,

transmitting data indicating programming to be decrypted together with said hash value to a program provider, and

said receiver additionally performs a third method comprising:

receiving a secret code from said program provider;

decrypting said secret code with said private cryptographic key stored in said data storage; and

storing a decrypted form of said secret code as said access data in said data storage.

2. The receiver of claim 1, wherein

said receiver additionally comprises a second microprocessor,

said data storage includes a read-only key register storing said private cryptographic key from which data is read only by said second microprocessor and a program control register, storing said hash value, to which data is written only by said second microprocessor, from which data is read by said first microprocessor,

said second microprocessor reads said computer readable serial number on said periodic basis, generates said hash value, and stores said hash value in said program control register, and

said first microprocessor reads said hash value from said program control register and transmits said data indicating programming to be decrypted together with said hash value to said program provider.

3. The receiver of claim 1, wherein

said data storage additionally stores a digital certificate, and

said digital certificate is transmitted with said data indicating programming to be decrypted.

4. The receiver of claim 1, wherein

said receiver comprises a plurality of components identified by computer readable serial numbers,

said first method includes generating a hash value representing each of said computer readable serial numbers and storing each of said hash values in data storage, and

said second method includes transmitting data indicating programming to be deciphered together with each said hash value to said program provider.

5. The receiver of claim 1, wherein said receiver performs said first method whenever said receiver is turned on.

6. The receiver of claim 1, wherein said second method additionally includes transmitting transaction data for purchasing additional program content.

7. The receiver of claim 1, wherein a portion of information transmitted to said program provider during performance of said second method is encrypted with a private key of said receiver.

8. The receiver of claim 1, wherein a portion of information transmitted to said program provider during performance of said second method is encrypted with a public key of said program provider.

9. A computer system for controlling access to encrypted programming transmitted to a plurality of receivers from a program provider, wherein said computer system comprises:

input means for receiving data signals from each receiver in said plurality of receivers;

output means for transmitting a secret code indicating a portion of said encrypted programming to be displayed by each receiver in said plurality of receivers;

data storage;

a processor; and

a database storing a data record for each receiver in said plurality of receivers, wherein each said data record includes a first data field identifying an address for sending data to said receiver, a second data field for storing a hash value for said receiver, and a third data field for storing a public cryptographic key of said receiver.

10. The computer system of claim 9, wherein said processor is programmed to perform a first method including:

receiving a message from a receiver in said plurality of receivers including data identifying said receiver, data indicating programming to be decrypted by said receiver, and a hash value;

identifying a data record within said database from said data identifying said receiver,

determining said hash value received in said message matches said hash value stored in said data record,

generating a secret code identifying programming to be decrypted by said receiver,

encrypting said secret code with a public cryptographic key of said receiver stored in said data record to form an encrypted version of said secret code; and

transmitting said encrypted version of said secret code to said receiver.

11. The computer system of claim 10, wherein

said data record additionally includes a fourth data field storing said secret code, and

said first method additionally comprises storing said secret code in said data record.

12. The computer system of claim 10, wherein said processor is additionally programmed to perform a second method including:

receiving a message from an additional receiver including data requesting registration with said computer system, data identifying said additional receiver, a public cryptographic key of said receiver, and a hash value;

establishing an additional data record within said database associated with said additional receiver;

storing said data identifying said additional receiver, said public cryptographic key of said receiver, and said hash value to said additional data record

generating a secret code identifying programming to be decrypted by said additional receiver;

encrypting said secret code identifying programming to be decrypted by said additional receiver with said public cryptographic key of said additional receiver to form an encrypted version of said secret code identifying programming to be decrypted by said additional receiver; and

transmitting said encrypted version of said secret code identifying programming to be decrypted by said additional receiver to said additional receiver.

13. The computer system of claim 12, wherein

said data record additionally includes a fourth data field storing said secret code, and

said second method additionally includes storing said secret code identifying programming to be decrypted by said additional receiver in said additional data record.

14. The computer system of claim 12, wherein

said computer system additionally includes data storage storing a data structure including a plurality of hash values of receivers received from one or more manufacturers of said receivers, and

said second method additionally includes determining that said hash value matches a hash value within said plurality of hash values before transmitting said encrypted version of said secret code identifying programming to be decrypted by said additional receiver to said additional receiver.

15. The computer system of claim 14, wherein said second method additionally includes determining validity of a digital certificate in which said public cryptographic key is transmitted.

16. The computer system of claim 12, wherein

said second data field stores a first plurality of hash values for said receiver,

said first method includes receiving a second plurality of hash values within said message from said receiver and determining whether said each of said second plurality of hash values matches a hash value within said first plurality of hash values, and

said second method includes receiving a third plurality of hash values within said message from said additional receiver and storing said third plurality of hash values in said additional data record.

17. The computer system of claim 12, wherein said first and second methods each additionally includes performing a transaction for purchasing program content.

18. A method for broadcasting program content from a program provider and displaying a portion of said program content at a receiver, wherein said method comprises:

a) generating a hash value within said receiver, wherein said hash value represents a computer readable serial number of a component within said receiver;

b) storing said hash value in data storage within said receiver;

c) reading said hash value from data storage,

d) transmitting data indicating programming to be decrypted together with data identifying said receiver and said hash value to a program provider,

e) finding a data record within a database accessed by said program provider including said data identifying said receiver;

f) matching said hash value transmitted from said receiver with a hash value stored within said data record;

g) generating a secret code identifying said programming to be decrypted;

h) encrypting said secret code with a public cryptographic key of said receiver stored within said data record to form an encrypted version of said secret code;

i) transmitting said secret code from said program provider to said receiver;

k) decrypting said encrypted secret code within said receiver with a private cryptographic key stored within said receiver; and

l) decrypting said portion of said program content with said secret code within said receiver.

19. The method of claim 18, wherein step d) is preceded by:

m) transmitting data indicating said receiver is to be registered with said program provider, said public cryptographic key of said receiver, and said hash value from said receiver to said program provider;

n) establishing an additional data record within said database accessed by said program provider; and

o) storing said data indicating said receiver is to be registered with said program provider, said public cryptographic key of said receiver, and said hash value from said receiver in said additional data record.

20. The method of claim 19, wherein step o) is preceded by:

p) receiving a plurality of hash values from one or more manufacturers of said receivers;

q) storing said plurality of hash values in a data structure accessed by said program provider; and

r) determining that said hash value transmitted by said receiver matches a hash value stored in said data structure.

21. The method of claim 20, wherein steps a) and b) are performed during initialization each time power is turned on at said receiver.

22. A computer readable medium storing program code causing a microprocessor controlling a receiver to perform a method including:

reading a hash value from data storage within said receiver,

transmitting data indicating programming to be decrypted together with said hash value to a program provider;

receiving a secret code from said program provider;

decrypting said secret code with a private cryptographic key stored in said data storage; and

storing a decrypted form of said secret code for use to decrypt program content in said data storage.

23. A computer data signal embodied in a carrier wave comprising program code causing a microprocessor controlling a receiver to perform a method including:

reading a hash value from data storage within said receiver,

transmitting data indicating programming to be decrypted together with said hash value to a program provider;

receiving a secret code from said program provider;

decrypting said secret code with a private cryptographic key stored in said data storage; and

storing a decrypted form of said secret code for use to decrypt program content in said data storage.

24. A computer readable medium storing program code causing a computer system to perform a method comprising:

receiving a message from a receiver in a plurality of receivers including data identifying said receiver, data indicating programming to be decrypted by said receiver, and a hash value;

identifying a data record within a database from said data identifying said receiver,

determining said hash value received in said message matches a hash value stored in said data record,

generating a secret code identifying programming to be decrypted by said receiver,

encrypting said secret code with a public cryptographic key of said receiver stored in said data record to form an encrypted version of said secret code; and

transmitting said encrypted version of said secret code to said receiver.

25. A computer data signal embodied in a carrier wave comprising program code causing a computer to perform a method comprising:

receiving a message from a receiver in a plurality of receivers including data identifying said receiver, data indicating programming to be decrypted by said receiver, and a hash value;

identifying a data record within a database from said data identifying said receiver,

determining said hash value received in said message matches a hash value stored in said data record,

generating a secret code identifying programming to be decrypted by said receiver,

encrypting said secret code with a public cryptographic key of said receiver stored in said data record to form an encrypted version of said secret code; and

transmitting said encrypted version of said secret code to said receiver.

26. A computer readable medium storing program code causing a computer system to perform a method comprising:

receiving a message from a receiver including data requesting registration with said computer system, data identifying said receiver, a public cryptographic key of said receiver, and a hash value;

establishing an additional data record within a database associated with said receiver;

storing said data identifying said receiver, said public cryptographic key of said receiver, and said hash value to said additional data record

generating a secret code identifying programming to be decrypted by said receiver;

encrypting said secret code identifying programming to be decrypted by said receiver with said public cryptographic key of said receiver to form an encrypted version of said secret code identifying programming to be decrypted by said receiver; and

transmitting said encrypted version of said secret code identifying programming to be decrypted by said receiver to said receiver.

27. The computer readable medium of claim 26, wherein said method additionally includes determining that said hash value received from said receiver matches a hash value within a plurality of hash values received from one or more manufacturers of said receivers before transmitting said encrypted version of said secret code identifying programming to be decrypted by said receiver to said receiver.

28 A computer data signal embodied in a carrier wave comprising program code causing a computer to perform a method comprising:

receiving a message from a receiver including data requesting registration with said computer system, data identifying said receiver, a public cryptographic key of said receiver, and a hash value;

establishing an additional data record within a database associated with said receiver;

storing said data identifying said receiver, said public cryptographic key of said receiver, and said hash value to said additional data record

generating a secret code identifying programming to be decrypted by said receiver;

encrypting said secret code identifying programming to be decrypted by said receiver with said public cryptographic key of said receiver to form an encrypted version of said secret code identifying programming to be decrypted by said receiver; and

transmitting said encrypted version of said secret code identifying programming to be decrypted by said receiver to said receiver.

29. The computer data signal of claim 28, wherein said method additionally includes determining that said hash value received from said receiver matches a hash value within a plurality of hash values received from one or more manufacturers of said receivers before transmitting said encrypted version of said secret code identifying programming to be decrypted by said receiver to said receiver.